

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)



Applicant's or agent's file reference CH920020013	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/IB 03/03187	International filing date (day/month/year) 07.07.2003	Priority date (day/month/year) 29.07.2002
International Patent Classification (IPC) or both national classification and IPC H04L9/32		
Applicant INTERNATIONAL BUSINESS MACHINES CORPORATION et al.		

- This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
- This REPORT consists of a total of 6 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

 These annexes consist of a total of sheets.

- This report contains indications relating to the following items:
 - I ☒ Basis of the opinion
 - II ☐ Priority
 - III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
 - IV ☐ Lack of unity of invention
 - V ☐ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
 - VI ☐ Certain documents cited
 - VII ☐ Certain defects in the international application
 - VIII ☐ Certain observations on the international application

Date of submission of the demand 23.02.2004	Date of completion of this report 09.12.2004
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Bec, T Telephone No. +49 89 2399-7124 

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/B 03/03187**

I. Basis of the report

1. With regard to the **elements** of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*):

Description, Pages

1-16 as originally filed

Claims, Numbers

1-12 as originally filed

Drawings, Sheets

1/5-5/5 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
☐ the language of publication of the international application (under Rule 48.3(b)).
☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
☐ filed together with the international application in computer readable form.
☐ furnished subsequently to this Authority in written form.
☐ furnished subsequently to this Authority in computer readable form.
☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/IB 03/03187**

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been examined in respect of:

☐ the entire international application,

☐ claims Nos.

because:

☐ the said international application, or the said claims Nos. relate to the following subject matter which does not require an international preliminary examination (specify):

☒ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. 1-12 are so unclear that no meaningful opinion could be formed (*specify*):

see separate sheet

☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.

☐ no international search report has been established for the said claims Nos.

2. A meaningful international preliminary examination cannot be carried out due to the failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions:

☐ the written form has not been furnished or does not comply with the Standard.

☐ the computer readable form has not been furnished or does not comply with the Standard.

Reference is made to the following document:

D1: XP010236752 "Self-certified identity information using the minimum knowledge"
HYUNG-KYU YANG and AL.

Re Item III

Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

The present application does not meet the requirements of Article 5 PCT.
The reasons being the following:

- (1) Independent claim 1 discloses "selecting a secret base value (g', h', x') in dependence on the modulus value (N)".

However it is seems that it is not disclosed in the description how the selection of the secret base value **in dependence** on the modulus is performed.

- (2) On page 10, line 21, the applicant has written "Given the secret cryptographic key sk_i ".

However neither the secret key sk_i nor the index " i " have been defined.

The applicant does not explain if the index " i " in the present case refers to the numbering of a server or the generation of a new key.

Moreover on page 9 the applicant has used the index " i " to refer to the index of an exponent (see formulas line 26), in line 21 he introduces sk_i and in line 23 he uses the index " i " twice in the formulae; as a result it is no longer clear to which element (exponent or key) the index refers and consequently it is not possible to implement practically the invention.

Furthermore the signature value is referred as " i ". Leading to an obscurity in the use of the letter " i " as to it's value.

The same comment applies as well to what is written on page 11.

- (3) The following symbols used in the description on page 10 and 11 have not been

defined:

- i) "⊕" page 10, line 25 and page 11, line 28.
 - ii) "H()" page 10 line 25 and page 11, line 27
- (4) The phrases "defining an order of the exponent values" and "publishing a description" are neither defined in the claims nor in the description.

Thus the present application does not meet the requirements of Article 5 PCT because the invention is not disclosed in manner sufficiently clear and complete to enable a skilled person to carry it out.

Notwithstanding the above mentioned points, the following on clarity should be noted:

- 1 The claims do not meet the requirements of Article 6 PCT as claims 1, 4, 7, and 8 have been written as independent method claims. It is actually noted that there could be a common inventive concept at this stage. The applicant is therefore asked to emphasized this concept by clearly linking the signature generation, verification and revocation method to the key generation method.

If the applicant fails or refuses to do so, non unity will be raised having regard to the disclosure of D1, D2 or D3 over the common technical features of claims 1, 4, 7 and 8 that are "the exponent values and a secret key".

- 2 It is clear from the description on pages 9, 10 and 11 that the following features are essential to the definition of the invention:

For independent claims 1, 4 and 7:

Deriving a public base value (g,h,x) from the exponent value:

(1) $g = g^{\prod_{i=1}^e p_i}$

(2) $h = h^{\prod_{i=1}^e p_i}$

(3) $x = x^{\prod_{i=1}^e p_i}$

For independent claims 4 and 7:

Deriving a second signature element from a provided secret cryptographic key (g',h',x'):

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/IB 03/03187

(4) $g_i^{ei} = g$

(5) $h_i^{ei} = h$

(6) $x_i^{ei} = x$

wherein the signature value is (i,y,a) with:

(7) $y = x_i g_i^a h_i^{a \oplus H(m)}$

For claim 7:

satisfy a known relationship with the message m:

(8) $y^{ei} = x g_i^a h_i^{a \oplus H(m)}$

Since these claims do not contain these features they do not meet the requirements of Article 6 PCT taken in combination with Rule 6.3(b) PCT that any independent claim must contain all the technical features essential to the definition of the invention.

- 2 The category of claim 12 is not clear as it discloses on one hand a network device but refers to the computer program of claim 11 (Article 6 PCT).
- 3 Although for the above reasons no fully reasoned opinion in respect of novelty and inventive step can be issued, it appears that the claims as presently drafted do not meet the requirements of Article 33(1) PCT having regard to the disclosure of D1 for example, see paragraph 4 and 5: